OutPut Total Security

User Guide

Last modified: May, 2014

© 2014 output. All rights reserved. Output™ is owned by mettlecorporation LLC. All other company and product names are trademarks of their respective owners.

OutPut Total Security includes anti-virus functionality (that detects and eliminates viruses, spyware, adware and other malware, worms, Trojans, rootkits and other threats) and the firewall that protects your work online.

Reliability of **OutPut Total Security** makes usage of the computer connected to Internet safer. OutPut Total Security, unlike many other antivirus software does not load the system and does not make conflicts with other installed products.

OutPut Total Security – is easy to use product, with minimal design and many useful functions, reliable and efficient at the time.

Download OutPut Total Security

Distribution **OutPut Total Security** is free for limited period and available from the project site http://www.outputtechnology.in

Installation OutPut Total Security

Proper installation of **OutPut Total Security** is provided by **OutPut Total Security** Installation Wizard. You just have to follow the wizard.

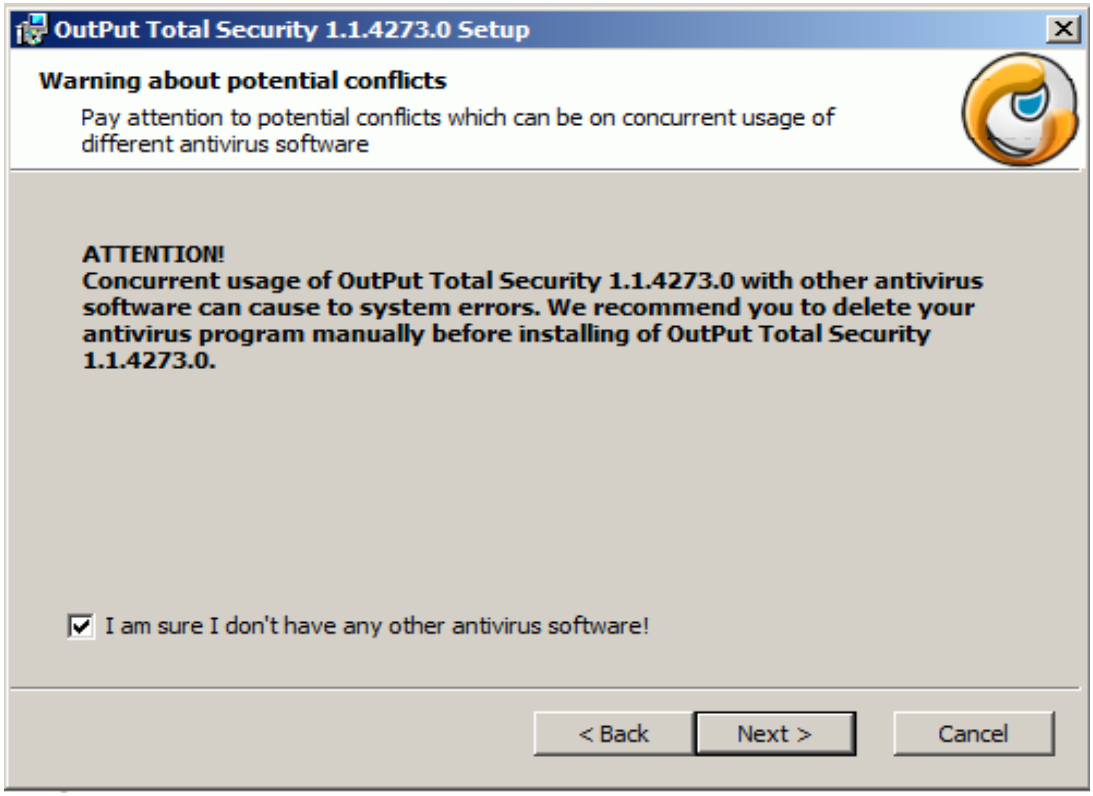
Prepare to install

Start the Installation Wizard

Read the license agreement and choose "I agree with the license agreement" if you agree with it, click "Next"

When installing **OutPut Total Security** you should pay attention to some important notes:

Before installing **OutPut Total Security,** the Installation Wizard emphasizes that the presence of other already installed antivirus software can cause conflicts in the operating system.


OutPut Total Security 1.1.4273.0 Setup
Warning about potential conflicts
Pay attention to potential conflicts which can be on concurrent usage of different antivirus software
ATTENTION!
Concurrent usage of OutPut Total Security 1.1.4273.0 with other antivirus software can cause to system errors. We recommend you to delete your antivirus program manually before installing of OutPut Total Security 1.1.4273.0.
I am sure I don't have any other antivirus software!
< Back
Next >
Cancel

There are several reasons that limit a usage of multiple antivirus products on the same computer:

- Anti-virus programs request the same system files as you work. Simultaneous requests to system resources can cause conflict or failure of system.
- Some antivirus products offer a scanning service in real time. Such scanning requires system resources. Your computer can start working much slower.

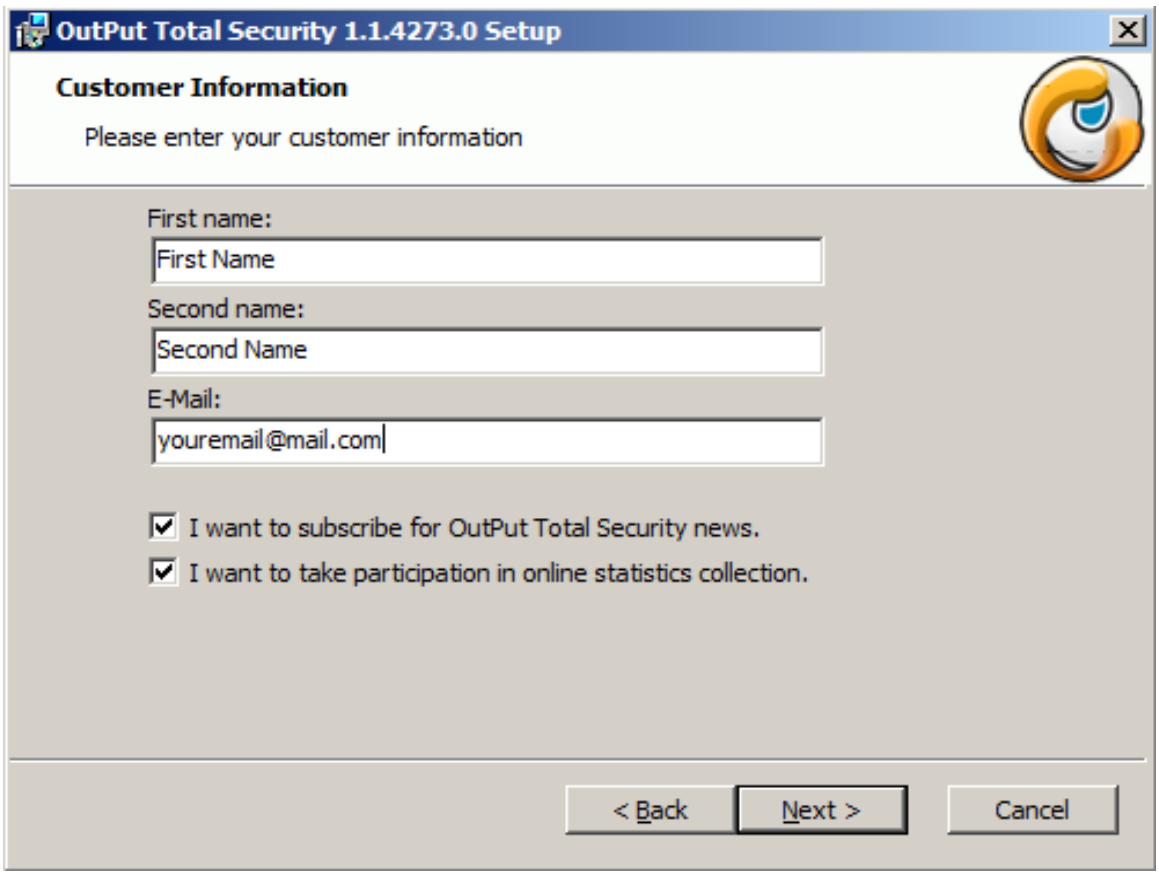
In addition, before installing **OutPut Total Security** you should remove its previous version.

To remove an old version of **OutPut Total Security** (anti-virus or a previous version) yourself, you should follow these steps:

1. Click **Start**, click **Control Panel** and double-click **Add or Remove Programs**.
2. Select an antivirus program to be deleted in the list of installed programs and click **Remove**.
3. For implementation of changes, follow the instructions on screen.

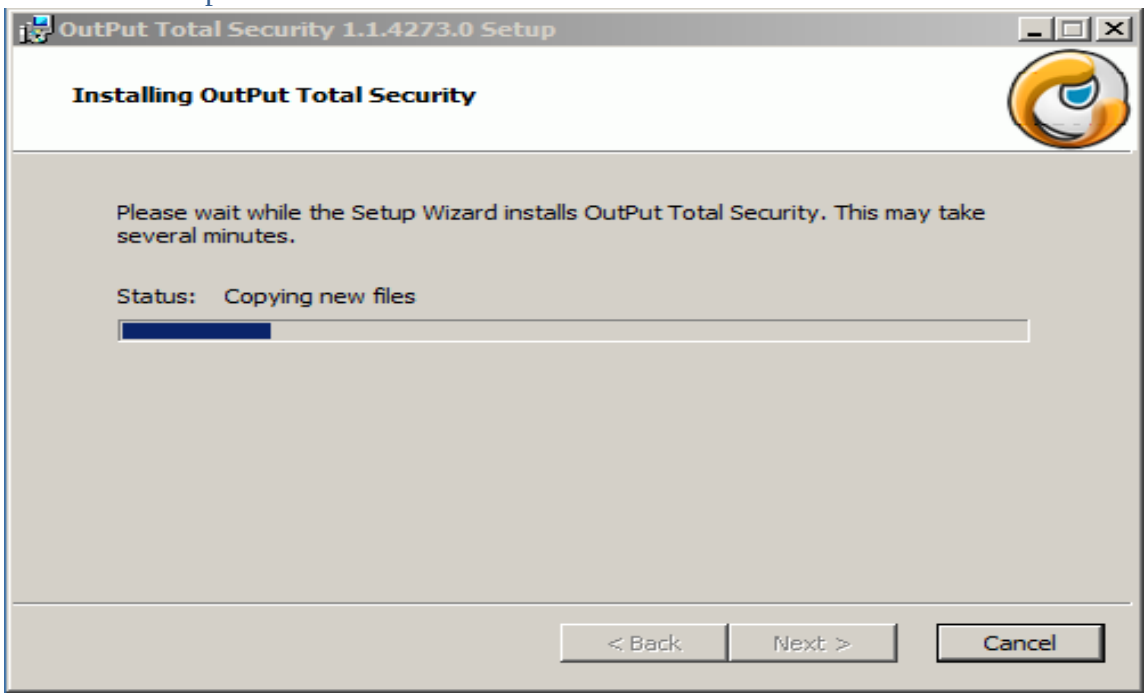
After removal of the previous anti-virus program, continue to follow the Setup Wizard.

Enter your name, email (anonymous information)

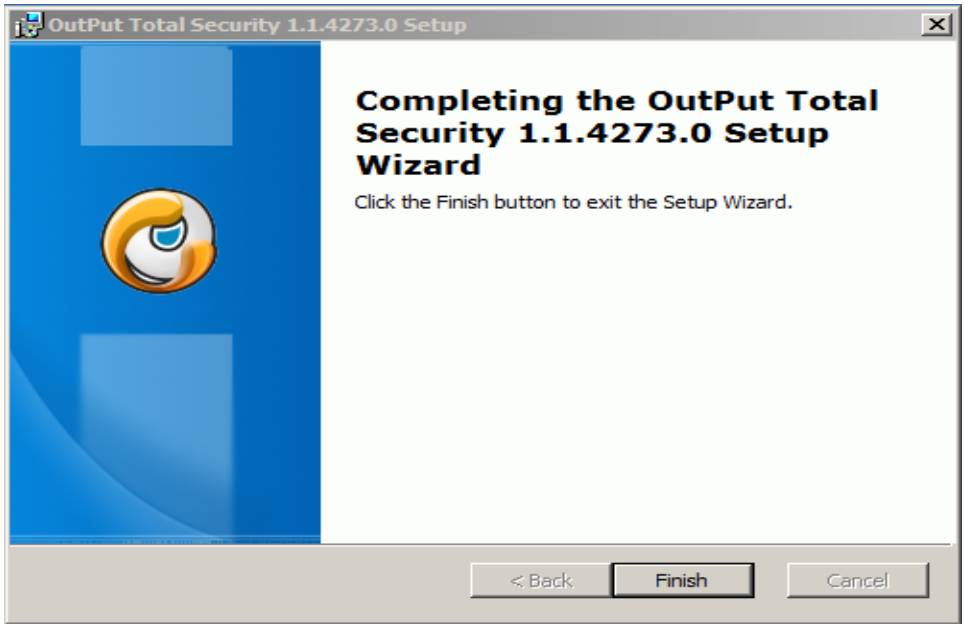


The installer is ready for installation. Click "Install"

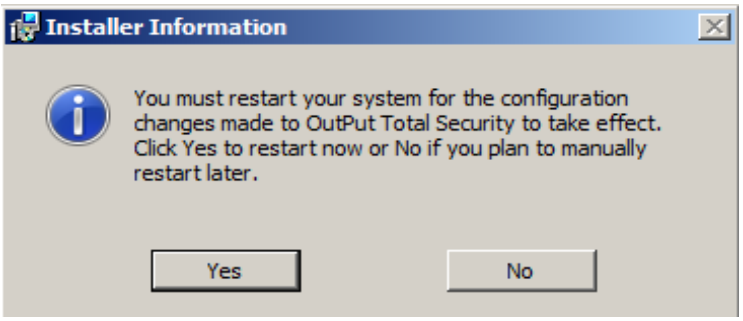
The installation process


OutPut Total Security 1.1.4273.0 Setup
Installing OutPut Total Security
Please wait while the Setup Wizard installs OutPut Total Security. This may take several minutes.
Status: Copying new files
< Back
Next >
Cancel

Installation completed successfully


OutPut Total Security 1.1.4273.0 Setup
Completing the OutPut Total Security 1.1.4273.0 Setup Wizard
Click the Finish button to exit the Setup Wizard.
< Back
Finish
Cancel

Restart the computer to successfully complete the installation


Installer Information
You must restart your system for the configuration changes made to OutPut Total Security to take effect. Click Yes to restart now or No if you plan to manually restart later.
Yes
No

System Status

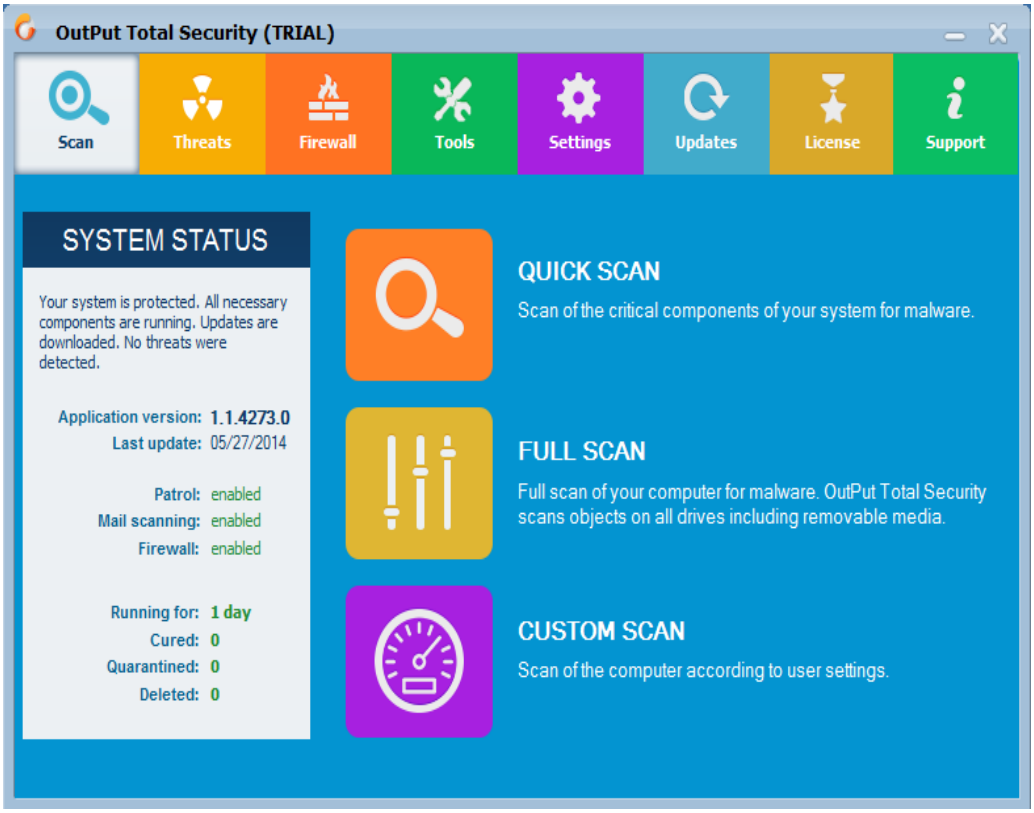
OutPut Total Security automatically monitors the system status in terms of security and provides summary information in the **System Status** in any window of the program.

OutPut Total Security presents graphical representation of the system status in two colors. Dark blue color indicates adequate protection for your computer: all systems for protection are on, anti-virus databases are up to date, and there are no active threats in the system at that time. The red color indicates the presence of security vulnerabilities (one or some modules of the product services are turned off, anti-virus database are outdated; there are currently active threats, etc.)

System Status area provides the description on the state of the system and the cause of security vulnerabilities and provides specific actions for their removal. You should only follow the advice and guidance offered by program by clicking **Fix** button.

System Scanning

OutPut Total Security has three scan modes, which are available in main window: **Quick**, **Full** and **Custom Scan**. Each set is provided with certain parameters of the mode.



Quick Scan – express scan of the most vulnerable sectors of system. The following objects are checked: system process, Windows system files, all files in Documents and Settings folder.

Quick Scan mode is useful in case of virus suspect after visiting suspicious site or in case when the system works incorrectly.

If you are not using **Patrol** function for some reasons, **Quick Scan** mode will be useful for regular periodic scanning, which you can configure to start automatically.

Full Scan – total system check thorough test of the system. The following items are scanned: system memory, objects that run on startup, backup storage systems, mail bases, hard, removable and network drives.

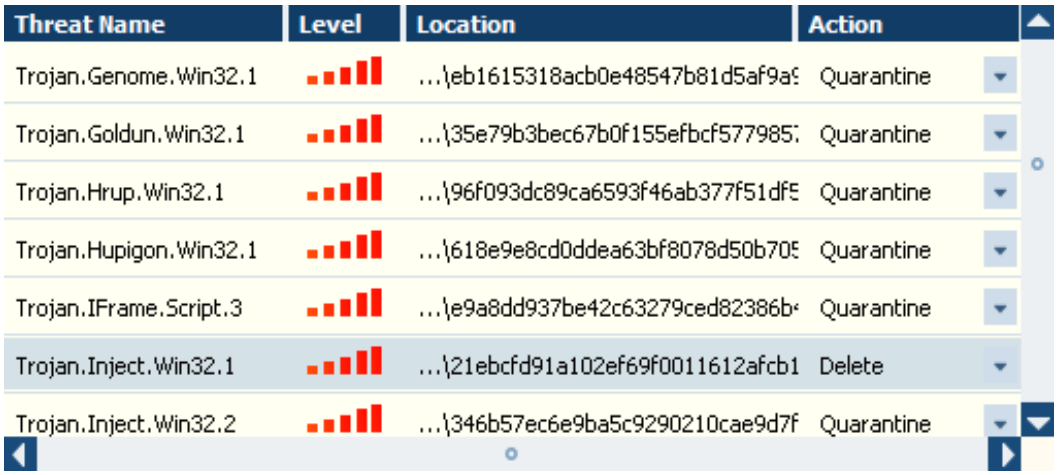
We recommend you to make a full system scan at least once a week. You should adjust full scan automatically not to forget about this important operation.

Custom Scan – scanning only files and folders that user wishes to check.

After the scan is complete, you will receive a detailed report on its results: total time of scanning and detailed information about the number of tested and infected objects.

If the threats are found there will appear a window with information about their names, level of threat and location and **OutPut Total Security** will offer an optimal action to neutralize infected files. In addition, you can choose a different action if you are sure that your decision is right.

When clicking the **Apply** button, **OutPut Total Security** will begin neutralization of all detected threats. This process can take several seconds to several minutes - depending on the number of detected threats. When this process is completed, you will receive a detailed report on the work done, which will contain the name of infected file and action, applied to it.



There are three levels of threats in **OutPut Total Security**:

FIRST LEVEL (green) - the files are found using heuristics.
SECOND LEVEL (yellow) – viruses that were found in archives, installation files, disk images, etc.
THIRD LEVEL (red) - infected files, which were found on the computer.

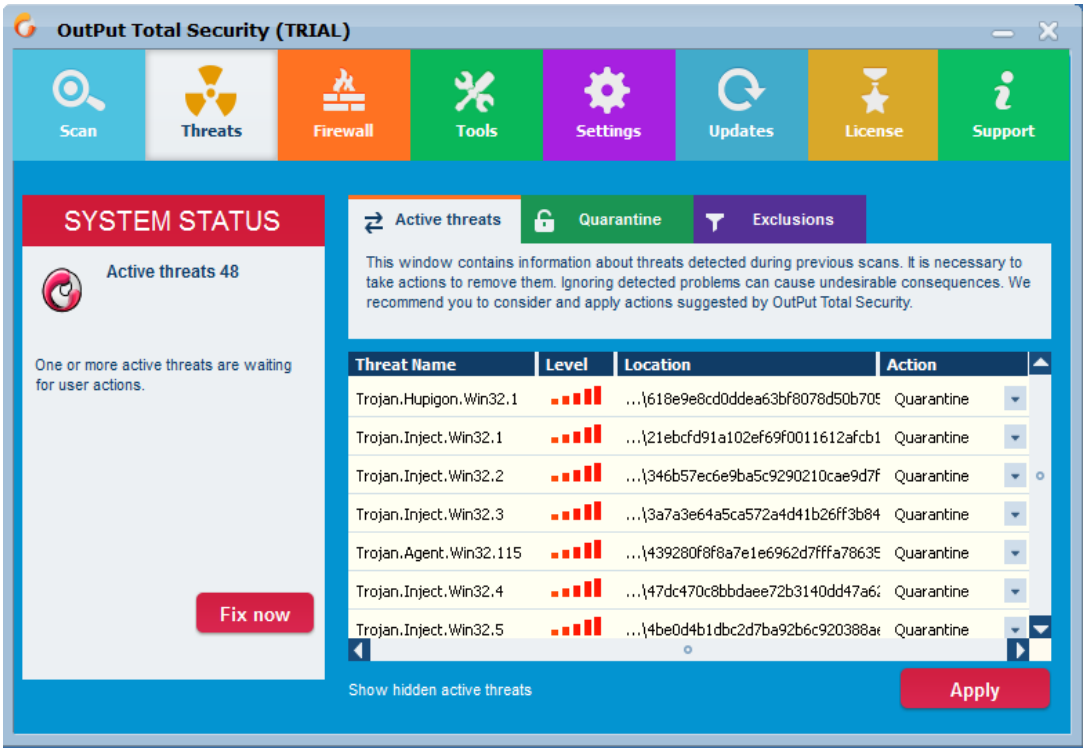
With **OutPut Total Security** you will not have to keep in mind the date of next scanning**.** You can configure to start scanning automatically using the **Scheduler**, which is available from the **Tools** menu.

If you do not have the time or will to wait for the scan is complete, you can use an option that is placed at the bottom of the SCAN window - "Turn off computer after scan."

When OutPut Total Security finds a threat

OutPut Total Security has a built-in algorithm of analysis of the identified threat and determination of the optimal action (hide/ignore/heal/quarantine/delete), which needs to be applied. After the scan is completed, in case of certain threats, you can view the actions, offered by the program.

In the **Threats** window you can view basic information about active threats (name, security level, location) and decide on their future fate.



You can change the reaction of anti-virus module for the object, if you are unsure in actions of antivirus. Otherwise, we recommend performing actions that the program offers.

Also you can **hide** active threats, if you are sure that your decision is right. In this case they will not be shown in the list of Active threats and influence the system status. However, we strongly recommend not doing that and better send suspicious files to our antivirus lab for the detailed study of the threat. To send suspicious files, choose **Tools -> Feedback.**

In some cases, to remove an infected object you have to restart your computer. So do not worry, if not all infected files can be deleted. However, in case when even after restart of computer the problem still exists, please seek help from customer service.

OutPut Total Security uses a special repository – **Quarantine -** to isolate dangerous files. We do not recommend you to restore files from quarantine, if you are not sure that they are safe.

OutPut Total Security has an option for **folders and files exceptions.** If you do not want some folders or files checked, you can put them to the list. It is possible that **OutPut Total Security** finds some malicious files are safe, so there was add an option to **Send files for analysis.** There is a note: only files are sent from the list of exceptions, folders are not sent to the laboratory for analysis. In case you've sent files which are not really harmful, experts will remove them from the base.

OutPut Total Security Preferences

You can configure the program on your own: choose objects to scan, actions to be performed in case of detection, configure the proxy server and more. If you are unsure about the correctness of your actions, we recommend using the default settings.

Settings of **OutPut Total Security** are divided into 3 categories: general, default actions and messages.

It is strongly recommended to always keep the option “Load at the launch of OS” activated: it will help **Output Total Security** to protect your system from the very first seconds of the PC launch.

When **OutPut Total Security** launches there appears a screensaver that disappears in a few seconds. If you do not want to see it every time you turn on your computer, you should clear the check mark in front of the corresponding field.

The following settings indicate which exactly is to be scanned: archive files, boot sectors, or turn on heuristics. It is recommended to leave a mark in front of each tag, to the maximum protection remained.

Heuristic analysis - is virus detection by typical behavior, i.e. the ability of antivirus software to identify a virus that just appeared, even if it is not added to the antivirus bases.

Option: "Load full set of base". This option is disabled by default. Antivirus is downloaded with a basic set of virus databases. The basic package includes the most world spread and dangerous viruses. If the antivirus finds at least one virus on your computer, it loads the full set of virus database (without rebooting antivirus).In complete virus database includes basic set and all the old and less ubiquitous virus signatures. In order to antivirus always worked with a full set of virus database you need to include this option in the settings and restart the antivirus.

OutPut Total Security has a built-in algorithm of heuristic analysis and therefore provides protection even against the latest viruses and threats.

Default actions of the Patrol. Specify what should be the reaction of **OutPut Total Security** when finding malicious file - from notification about its presence to its removal, the **Firewall mode** determines a way of the establishment of rules to network access for programs: Automatic, Interactive (by user).

When the Message section is set, **OutPut Total Security** will notify you about the detection of infected or suspicious files in email messages, as well as about the completion of the upgrade process.

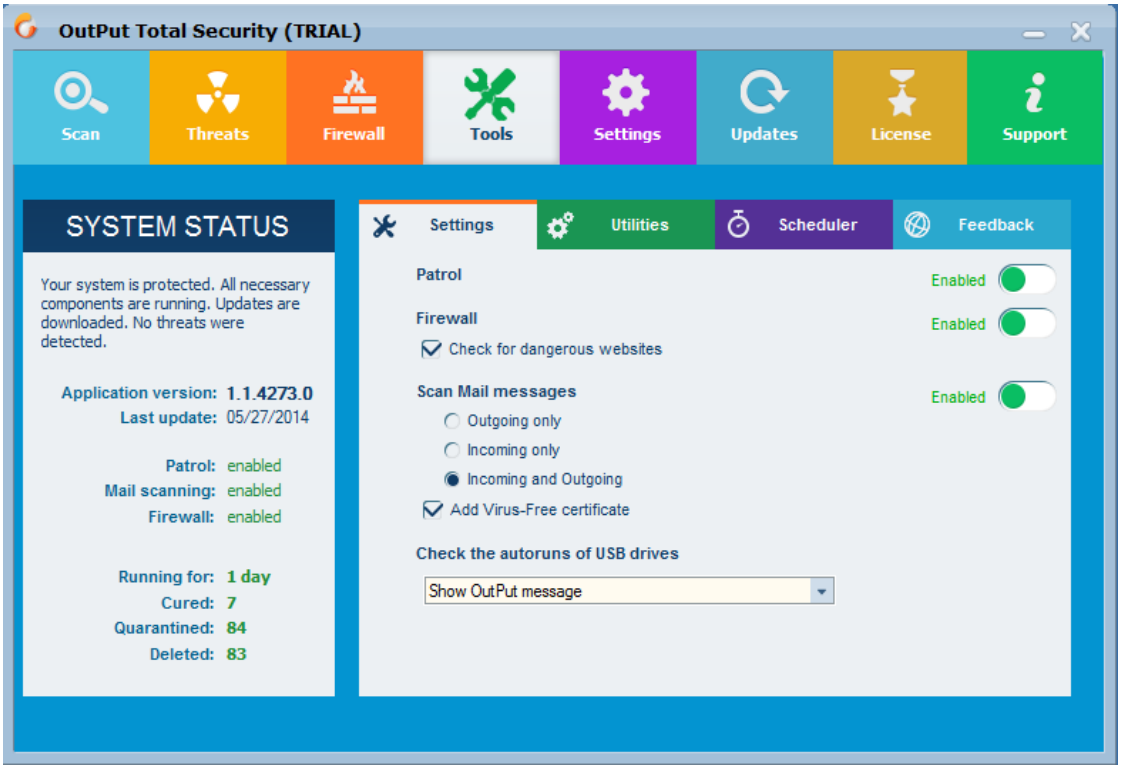
Real time system protection

OutPut Total Security has a built-in tracking in real time, entitled **Patrol. Patrol** detects viruses and other malicious programs "at the moment", effectively blocking them even before the entry into the operating system or files, tracks running processes and thus ensures reliable prevention of infection.

By default, the **Patrol** is automatically activated every time you start the program. This is a very important component of protection. We do not recommend you disable this feature. To check whether the **Patrol** is turned on, press the right mouse button on **OutPut Total Security** icon in the taskbar notification area or go to the **Tools -> Properties.**

OutPut Total Security protection components

To guarantee a multilevel protection, except **Patrol**, **OutPut Total Security** has several important components:



- **Office documents check**

OutPut Total Security checks all types of Microsoft Office documents.

- **Check the files that are downloaded to a computer with Internet**

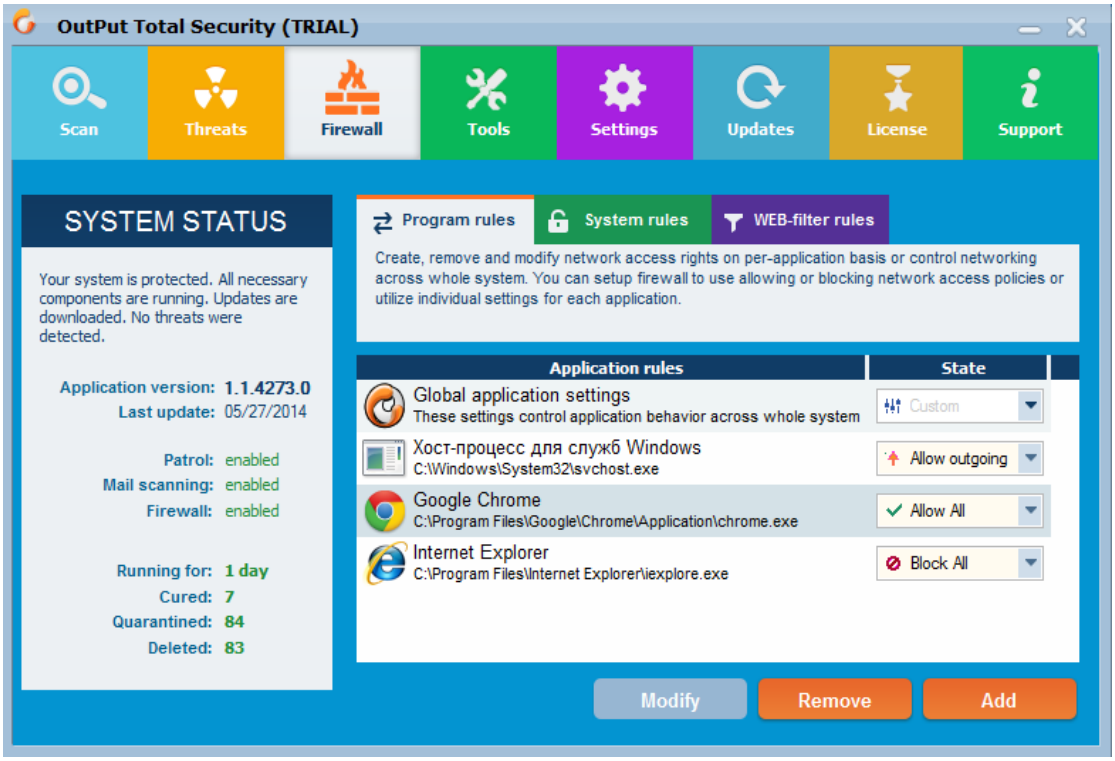
OutPut Total Security monitor all users download from the Internet and after the detection of malicious files blocks them.

- **Mail check**

Mail filter checks all incoming and outgoing mail messages and attachments, which guarantees computer safety.

- **Firewall**
  This module is very important if there is a network or Internet in your PC.

A firewall monitors all attempts of application to access the network - both incoming and outgoing traffic;



- **Protection against external attacks.**
  By default, Firewall allows applications only outbound connections. This allows to protect system against malicious attempts to take control over it.

- **Built-in set of rules**.
  Application has built-in set of rules that have all necessary rules to allow functioning of standard system services and protocols (NetBios, DHCP, DNS etc.) With these rules network activity of particular protocol or service could be easily enabled or disabled.

- **An ability to set global settings for all applications in the system**.
  OutPut Total Security has an opportunity to set global settings for all applications. For example, if you need to give an access to server for all applications. To do that, you can set a rule to allow access to certain IP-addresses on port settings. In addition, there will be no need for each application to create separate rules for access to this server.

- **WEB-filter**. Blocking of dangerous sites and malicious content. **OutPut Total Security** has an ability to block malicious content from untrusted sites in browser. In this case, user is shown a message. If the site is in a "black list", you will be able to attend it, view the images, but not be able

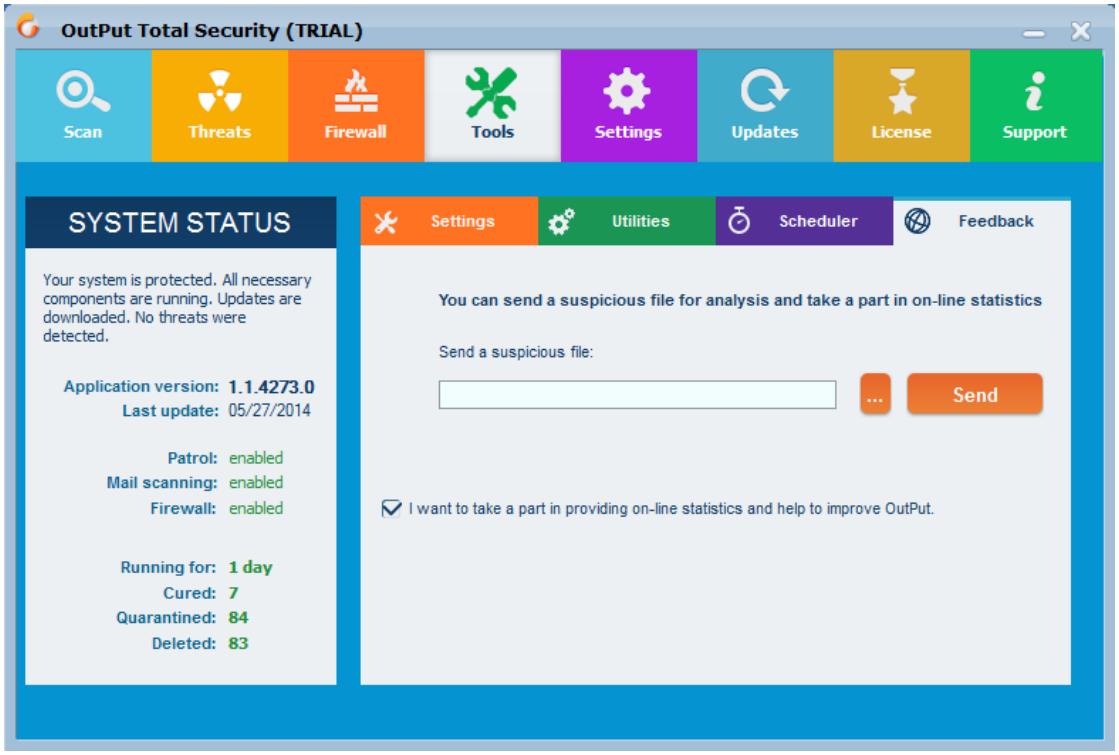
to download programs, archives, documents and other files that could potentially harm your computer from this site.

- **Additional Utilities: Task Manager and Startup Manager**

Additional tools such as Task Manager and Startup Manager expand the functionality of the program and help user to control processes in the system better. Task Manager is required to watch applications that run on your computer, and control them. Using Startup Manager you can view information about programs that start automatically when you start Windows.

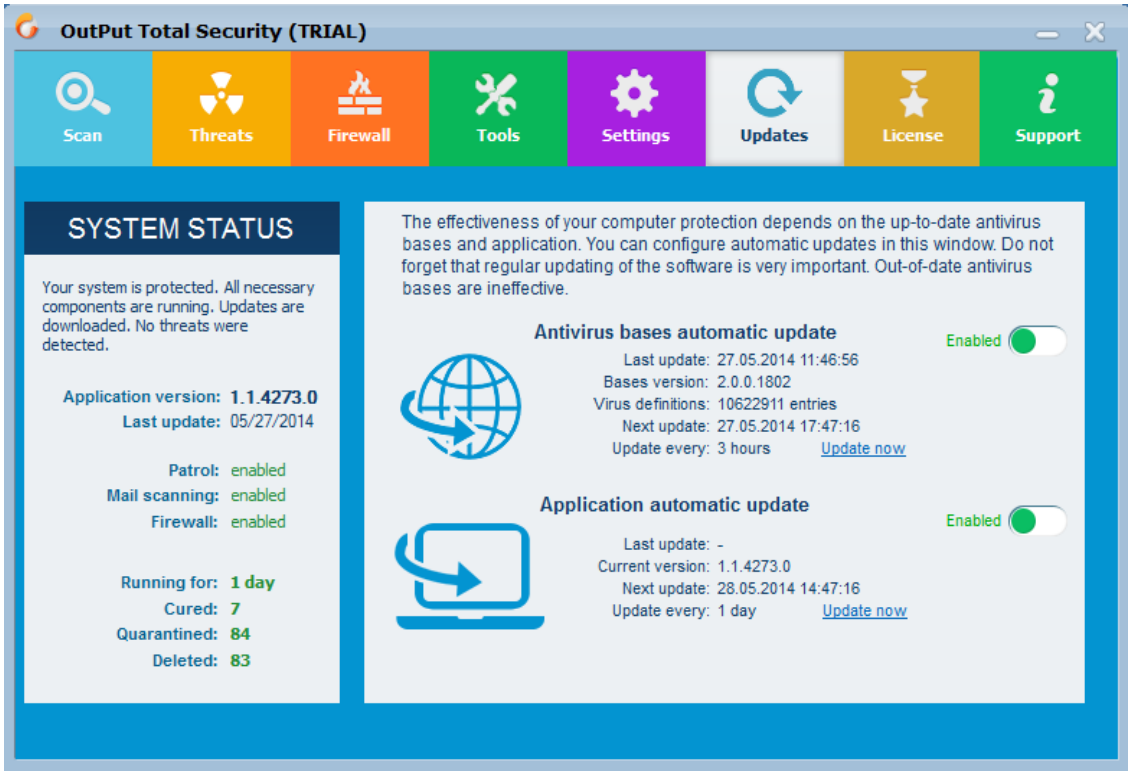
- **Feedback**

If you have suspicions about certain files, you can send them to our laboratory and participate in collecting statistics. Thus, you can help us respond more quickly to new threats and updating existing ones.



Databases and program modules updates

The effectiveness of antivirus product depends on how regularly virus database is updated. Regular automatic update of databases is critically needed to keep the optimal level of protection of your computer.



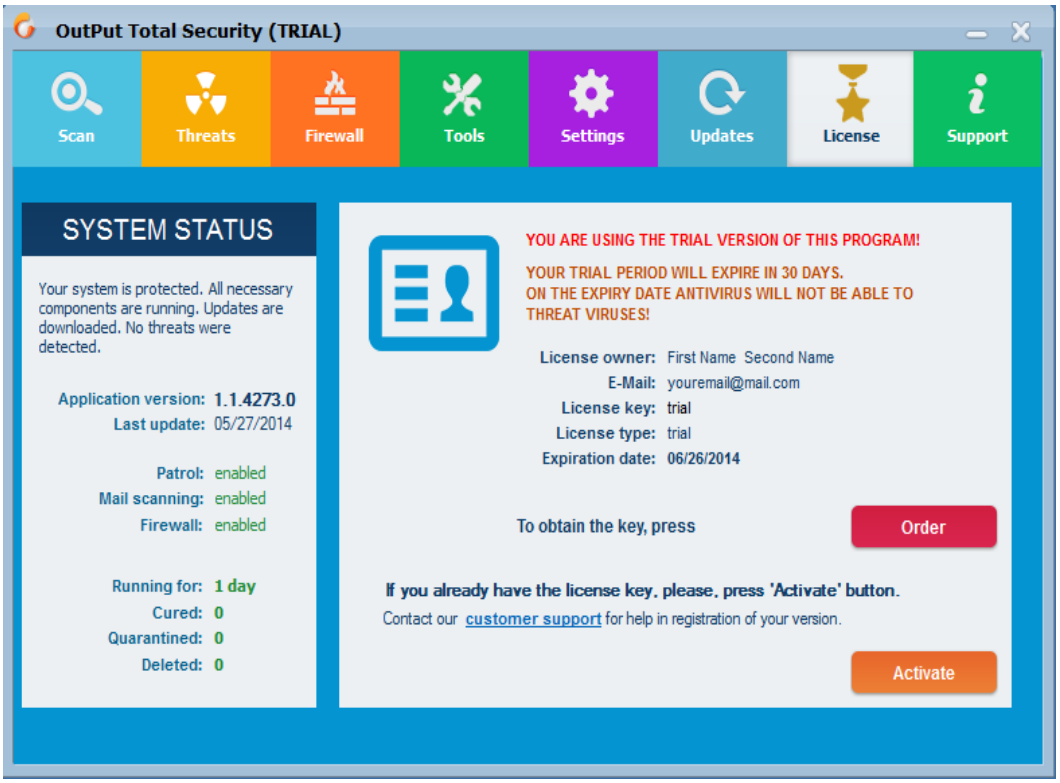
Developers of **OutPut Total Security** promptly react to new threats, update the antivirus bases and bases of malware. Typically, virus updates are issued 1-2 times a day. In case of epidemics OutputTechnologies team prepares updates in accelerated mode to protect users.

For users who do not have regular access to the Internet, it is possible to use off-line updates of anti-virus.

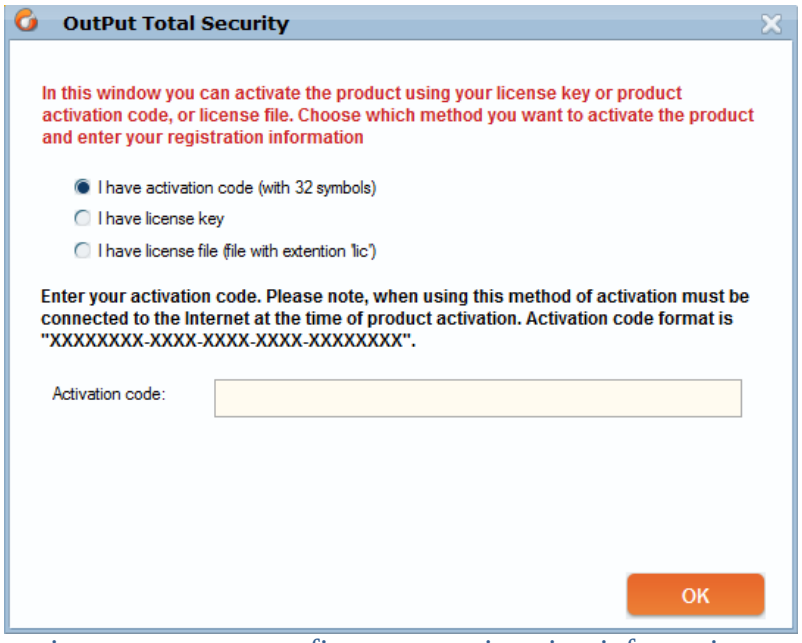
By default, automatic database updates and program modules are enabled. If for any reason you need to disable these settings, return to their original state as soon as possible.

OutPut Total Security registration

This is how unregistered program window looks like:



To register the program, enter/copy the code, which you purchased, to the “License code” box on “License” tab and click "Activate".


OutPut Total Security
In this window you can activate the product using your license key or product activation code, or license file. Choose which method you want to activate the product and enter your registration information
I have activation code (with 32 symbols)
I have license key
I have license file (file with extention 'lic')
Enter your activation code. Please note, when using this method of activation must be connected to the Internet at the time of product activation. Activation code format is "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX".
Activation code:
OK

You will receive a request to confirm your registration information, and then fill in correct information and click “Send”

OutPut Total Security will inform you about the successful registration.

Customer support

If you have questions about **OutPut Total Security**, you can contact customer support service.

Users can use the following:

- E-mail - support@outputtechnology.in
- Fill in the request form to customer service.

Direct all legal questions about this Agreement to: LEGAL@OUTPUTTECHNOLOGY.IN.

ALL MATTERS SUBJECTED TO BANGALORE (INDIA) JURISDICTION

THE SOFTWARE IS PROTECTED BY INTELLECTUAL PROPERTY LAWS AND INTERNATIONAL TREATY PROVISIONS. UNAUTHORIZED REPRODUCTION OR DISTRIBUTION IS SUBJECT TO CIVIL AND CRIMINAL PENALTIES.